

**UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
ALEXANDRIA DIVISION**

Project Honey Pot, a dba of Unspam  
Technologies, Inc.,

Plaintiff,

v.

Andrey Chernuk and Boris Livshits  
dba Toronto Pharmacy,

Defendants.

No. 1:11CV15 LMB/JFA

**PLAINTIFF'S RESPONSE TO ORDER TO SHOW CAUSE RE: RULE 4(M) &  
MEMORANDUM IN SUPPORT OF PLAINTIFF'S MOTION TO EXTEND RULE 4(M) DEADLINE TO  
SERVE DEFENDANTS**

On May 11<sup>th</sup>, this Court ordered plaintiff to show cause why this case should not be dismissed based on Rule 4(m). Plaintiff herein responds to that order, explaining why the case should not be dismissed, but should be allowed to proceed against the newly named defendants – Andrey Chernuk and Boris Livshits. These named defendants are the owners of an illegal online pharmacy doing business under the trade name Toronto Pharmacy, and are advertising their illegal business through fraudulently transmitted spam, including spam directed toward Project Honey Pot. As explained below, the defendants have gone to great lengths to avoid being identified as the owners of Toronto Pharmacy and avoid being tied to the spam emails transmitted to Project Honey Pot. Despite defendants' efforts to hide, Plaintiff has diligently investigated the facts behind this case, and is now prepared to serve both defendants (at private mail box/mail forwarding services they are using in Florida) and proceed with its case

against them. Defendants will suffer no prejudice from an extension of the Rule 4(m) deadline, but plaintiff would suffer prejudice if the case were dismissed.

For all these reasons, Plaintiff Project Honey Pot respectfully requests an order extending its Rule 4(m) deadline to serve the defendants to June 15.

### **FACTUAL BACKGROUND**

As noted in the Complaint, spam is a global problem of epidemic proportions. In the six years it has been collecting data prior to the filing of this lawsuit, Project Honey Pot has already received well over 1 billion spam messages. Sorting this many spam messages into discrete bundles and tying those bundles to responsible parties is an extremely difficult and time consuming process. But it is not impossible.

All spam messages carry with them certain data point “fingerprints” that can be used to track the message back to those responsible for sending it. These data points can be any number of factors (including data contained in the spam message itself or data not contained in the message but tied to it in some way). Examples of data points can include: the IP address sending the message, a unique subject line or message body, or (most importantly) some payment information tied to the purchase of some essential service bought by the spammer to enable his spam transmissions. Unfortunately, spammers know they leave fingerprints behind, and go to great lengths to hide the most useful fingerprints (such as payment information) and to alter even trivial fingerprints to make it harder for investigators to rank spammers based on the size of their message bundles.

Defendants Chernuk and Livshits are no different from every other spammer in this regard. Over several years, they have systematically advertised their online pharmacy doing business under the name Toronto Pharmacy. But in sending their spam, they have constantly

altered their fingerprints. They are using compromised computers to send their spam, which means the originating IP addresses of their spam varies with each machine they illegally use. In addition to hiding their point of origin, they also alter the website address being advertised. Unlike legitimate marketers who consistently advertise one website to build brand awareness, these defendants advertised thousands of different websites hosted within around 170 different domain names. These domain names are largely purchased from registrars outside the United States, and are hosted on servers also located outside the United States. All the public information tied to these domain names is falsified or hidden behind private registrations.

Over the past several years, Project Honey Pot has focused a tremendous amount of its investigative resources tracing pharmacy spam. Such spam is perhaps the most pernicious and damaging, as well as the most lucrative for the spammers. Those responsible for pharmacy spam are little more than high-tech drug traffickers. They sell counterfeit or fake prescription drugs to unwitting consumers without the benefit of a reputable doctor's prescription. They sell their drugs at prices typically well below those charged by brick and mortar drugstores that are managed by licensed pharmacists (who are closely regulated by state and federal authorities and who dispense authentic drugs tested and approved by the FDA).

The harm caused by these drug-trafficking spammers is real. A number of public reports have focused on the growing problem of pharmacy spam, the injuries traced to it, and the difficulties encountered by those who try to identify the killers behind the business.<sup>1</sup>

---

<sup>1</sup> *SpamIt, Glavmed Pharmacy Networks Exposed*, Krebs On Security, February 2011 (available at <http://krebsonsecurity.com/2011/02/spamit-glavmed-pharmacy-networks-exposed/>); *The Partnerka: What Is It and Why Should You Care?* D. Samosseiko, 2009 (available at: <<http://www.sophos.com/security/technical-papers/samosseiko-vb2009-paper.pdf>>); *Pharmacists Warn of Buying Drugs Online After Death Reported*, CBCNews.com, March 21, 2007 (available at <<http://www.cbc.ca/canada/british-columbia/story/2007/03/21/drugs-online-warning.html>>); *Spam Hunter*, Forbes.com, July 23, 2007 (available at <[http://www.forbes.com/business/free\\_forbes/2007/0723/054.html](http://www.forbes.com/business/free_forbes/2007/0723/054.html)>) (profiling the unsuccessful attempts by the head of technology at a major spam-filtering company to track pharmacy spam to its source).

Project Honey Pot's work against pharmacy spam has produced useful results. We have identified tens of thousands of different domain names appearing in spam that lead to online pharmacies operating under questionable circumstances. We have mapped those domain names to fewer than 200 specific Internet "fingerprints."<sup>2</sup> Most importantly, nearly 90% of all this activity can be mapped to less than two dozen fingerprints, and approximately half of these fingerprints are connected to only one "hand"<sup>3</sup> that represents over 50% of the entire online pharmacy spam problem today. Defendants Chernuk and Livshits represent one discrete finger on this hand.

Despite doing all that they can to hide, defendants Chernuk and Livshits have now been named and sued by Project Honey Pot for their role as the owners of Toronto Pharmacy, and thus responsible for the millions of global spam messages advertising its numerous websites. Project Honey Pot has also just recently determined that both defendants are now using private mailboxes in Florida to receive mail on their behalf. Plaintiff is now prepared to move swiftly to serve these defendants at these addresses and proceed with its case against them.

The defendants will not be prejudiced in any way by an extension of the deadline to serve under Rule 4(m). The case is still in the beginning stages and the defendants have expended no resources in preparing a defense in the case to date (as far as Plaintiff is aware).

In contrast, Project Honey Pot would be prejudiced by a dismissal of the case. Project Honey Pot has expended substantial resources gathering information on these defendants and has paid a filing fee in this case that would be lost if the case were to be dismissed.

---

<sup>2</sup> As mentioned above, a "fingerprint" consists of any set of data that is likely to uniquely define a spam operation, and that serves to distinguish it from other spam operations. The data we consider includes the domain name hosting the site, the look and feel of the site, the technical data underlying the site, and any data points about the site that we may acquire through subpoena or other investigative means.

<sup>3</sup> A "hand" is a collection of unique fingerprints that nonetheless have apparent connections between them. In our experience, different fingerprints join together on the same hand when different spammers conspire with each other in some material way. They may be sharing resources, or using common vendors or suppliers, or sharing tricks of the trade between them that are not in common use throughout the criminal spam world.

Although the fee is not large, it is still a cost that must be paid in advance by plaintiffs like Project Honey Pot who are trying to address the spam problem.

### **LEGAL ARGUMENT**

Federal Rule of Civil Procedure 4(m) provides that a plaintiff who shows good cause for failure to effectuate service within 120 days of filing the complaint is entitled to an appropriate extension of time to serve. Courts have held that good cause exists – and that a plaintiff is entitled to additional time to effect service – when defendants take affirmative actions to avoid service of process. For example, in Ruiz-Varela v. Velez, the District Court dismissed the plaintiff's complaint pursuant to Rule 4(m) for failure to serve Defendant Figueroa. 814 F.2d 821 (1st Cir. 1987). Recognizing that Figueroa was attempting to evade personal service by concealing his whereabouts, the First Circuit vacated the dismissal. Because Figueroa's attempts to conceal his location were designed to frustrate the plaintiff's ability to effectuate service, the Court of Appeals explained that dismissal for failure to serve was inappropriate: “Evasion of service by a putative defendant constitutes good cause for failure to serve under Rule 4[m].” *Id.* at 824. As noted above, defendants Chernuk and Livshits in this case have gone to extreme measures to evade identification, and, thus, service of process. Their attempts at evasion are an adequate basis for extending Project Honey Pot's deadline to serve.

This Court should also grant Project Honey Pot an extension of time to serve the defendants due to its diligence in prosecuting this matter. Courts have consistently held that “a showing of diligence and a reasonable effort to effect service” constitute good cause under Federal Rule of Civil Procedure 4(m). In re Hall, 222 B.R. 275, 279 (Bankr. E.D. Va. 1998) (citing T & S Rentals v. United States, 164 F.R.D. 422, 426 (N.D. W.Va. 1996) and United States v. Britt, 170 F.R.D. 8, 10 (D. Md. 1996)). In determining the type of diligence or extent of

effort required to warrant an extension of the 120-day deadline, courts have examined the legislative history of amendments to Rule 4, noting that: “Inadvertent or heedless non-service is what amended Rule 4[m] is aimed at. Congress intended that a plaintiff who had made reasonable efforts to effect service would be permitted additional time, if needed, under Rule 6(b).” Arroyo v. Wheat, 102 F.R.D. 516, 518 (D. Nev. 1984) (citing to cases in which “there was no dilatory or willful delay” and in which “plaintiff’s abortive efforts [were] bona fide,” as illustrative of situations in which “good cause” was determined to exist); see also Quann v. Whitegate-Edgewater, 112 F.R.D. 649, 659 (D. Md. 1986) (citing Arroyo v. Wheat).

Project Honey Pot has analyzed millions of spam messages and hundreds of thousands of websites to identify the patterns leading to Toronto Pharmacy, and has worked diligently to trace this spam back to defendants Chernuk and Livshits. Project Honey Pot has also worked closely with other victims of these defendants (and pharmacy spam generally) in an effort to ensure its work does not inadvertently compromise other pending civil and criminal investigations.

All of these reasons constitute good cause for a short extension of the deadline to serve defendants Chernuk and Livshits in this case.

///

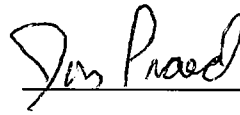
///

///

**WHEREFORE**, for the foregoing reasons and any additional reasons that may be adduced on this matter, Project Honey Pot respectfully asks the Court not to dismiss this case, and to grant its motion to extend to June 15<sup>th</sup> its deadline to serve the defendants. A proposed Order has being submitted for the Court's consideration.

Dated: May 19, 2011

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Jon Praed", is written over a horizontal line.

Jon L. Praed  
VSB #40678  
Attorney for Plaintiff Project Honey Pot  
Internet Law Group  
4121 Wilson Boulevard, Suite 101  
Arlington, Virginia 22203  
Phone: (703) 243-8100  
jon.praed@i-lawgroup.com